UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/519,827	12/21/2005	Michael Jacobs	CHAP-005	3097

36822 7590 07/20/2010

GORDON & JACOBSON, P.C.
60 LONG RIDGE ROAD
SUITE 407
STAMFORD, CT 06902

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
07/20/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/519,827	JACOBS, MICHAEL	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 April 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *63-68* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *63-68* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

FINAL ACTION

1. This action is in response to amendment filed 4/27/2010. Claims 69-72 are cancelled. Claims 63-68 are pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 63-66 are rejected under 35 U.S.C. 103(a) as being unpatentable over Toh (US Patent Publication No. 2002/0004902) in view of Haber et al. (US Patent No. 5,781,629 and Haber herenafter).

3. As to claim 63, Toh teaches a method of permitting authentication of data comprising: (a) storing copies of a plurality of data items (e.g., ... local storage [par. 36]); (d) transmitting said single hash value to a remote location (e.g., Operation Center) (i.e.,... teaches sending encrypted hash of the data package to Operation Center [par. 58]), via an information technology communications network [fig. 2];

Toh does not teach: (b) generating a first data file comprising a respective hash value of each said plurality of stored data items; (c) generating a single hash value of said first data file derived from said hash values of said plurality of stored data items; (e) creating at said remote location a second data file comprising said single hash value and one or more additional data items relating to said single hash value; (f) generating a hash value for said second data file; and (g) publishing said hash value for said second data file in a journal for authenticating said second data file. (h) authenticating said second data file by generating a hash value for said second data file and comparing the hash value for the second data file generated in (h) with the hash value for said second data file published in said dated journal.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Toh as introduced by Haber. Haber discloses: (b) generating a first data file comprising a respective hash value of each said plurality of stored data items (to generate a data structure (e.g., table) comprising hash values of data items [col. 5, lines 52-56]); (c) generating a single hash value of said first data file derived from said hash values of said plurality of stored data items (to generate a single hash linked to a number of hash values [col. 3, lines 60-67]); (e) creating at said remote location (e.g., service bureau) a second data file comprising said single hash value and one or more additional data items relating to said single hash value (to provide

the capability to create a second document (e.g., second data file) at a remote location [col. 5, lines 44-48]);

(f) generating a hash value for said second data file (to provide the capability to generate a hash value for the second document [col. 5, lines 45-50]). (g) publishing said hash value for said second data file in a journal for authenticating said second data file (to provide the capability to publish a hash value [col. 6, lines 45-60]). (h) authenticating said second data file by generating a hash value for said second data file and comparing the hash value for the second data file generated in (h) with the hash value for said second data file published in said dated journal (to provide authentication capability involving computing a hash a secondary hash of a stored data item [col. 6, lines 65-67; col. 7, lines 1-5]).

Therefore, given Toh's ability to transmit a hash to a remote location, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Toh to enhance hash maintainability by employing the well known feature of publishing hash values as disclosed above by Haber.

4. As to claim 64, Toh teaches a method where said first data file is generated in (b) at the end of a predetermined time period (par. 86).

5. As to claim 65, Toh teaches a method where: said first data file (e.g., delivery) contains at least one identifier selected from the group consisting of a Application/Control Number: 10/519,827 Page 11 Art Unit: 2431 file name, a path name, a file size and a time stamp (i.e., ... teaches delivery content including header information (e.g., address information) [par. 67]).

6. As to claim 66, Toh teaches a method where least one of said first data items comprises a message to be transmitted from a sender to a receiver [par. 67].

7. Claims 67 and 68 are rejected under 35 U.S.C. 103(a) as being unpatentable over Toh.

8. As to claims 67, Toh teaches a method further comprising: the sender generating a first hash value of said message (i.e., ...teaches the sender generating a hash value of the data to be transmitted [par. 58]); the sender encrypting said message with a first secret key and producing a second hash value from said encrypted message (i.e., .. teaches performing an encryption operation before sending the message [par. 58]); the sender encrypting said first secret key with a second secret key (i.e., ...teaches the receiver receives an encrypted document decryption key [par. 67]); the sender transmitting to the receiver said encrypted message, said encrypted first secret key (e.g., encrypted document decryption key) and said first hash value (i.e., .. teaches the sender

sending the encrypted data [par. 67] ...the encrypted data comprising a message, a decryption key, and hash value [par. 67]); the sender transmitting said second hash value and said second secret key to a third party (i.e., ...teaches a third party receives an hash value and encrypted message [par. 58]); the receiver (e.g., OC) receiving said encrypted message and generating a purported copy of said second hash value of said encrypted message (i.e., ...teaches the receiver receiving the encrypted message, decrypting the message and performing a hash operation [par. 67]); the third party determining whether the purported copy matches said second hash value (i.e., ..teaches a third party comparison operation between hashes [par. 58]); and the third party then releasing said second key if a match is so determined (i.e., ...teaches upon successful verification of hash key information then delivered to the recipient [par. 67]).

Toh does not expressly teach as claimed: the third party storing the transmitted second hash value and second secret key for audit purposes; However given Toh's disclosure of a third party performing a hash operation for the purpose of validation comparison, this would imply to those skilled in the art that Toh would have to have previously stored a hash value in order to have a hash value to compare too [par. 58].

Therefore this would also imply that inherent to Toh's hash capability is Toh's ability to store a given hash value at a third party. The audit element of applicant's claim limitation indirectly is related to Toh disclosing the ability to

maintain hash values for the purpose of validation comparison. Also, Toh does teach storing key data (e.g., secret key) [par. 69]. The key data Toh discloses is from both sender and receiver. Therefore given the implied teachings of Toh in this regard, one of ordinary skill in the art would recognize the benefit of storing hash values to enhance the hash comparison process. Toh does not expressly teach as claimed: the receiver transmitting the purported copy of said second hash value to the third party, However Toh does disclose the ability to exchange data between a receiver and third party for verification purposes and the ability for the receiver to perform a hash operation on received data (e.g., second hash value) [par. 39 & 67]. (The Examiner notes that the specification lacks a specific example to clearly interpret this limitation and as such the Examiner has interpreted this limitation under the broadest reasonable interpretation and consistent with what is common in the art). Consistent with what is known in the art, a third party in a message exchange system is commonly used for authentication or privacy. Therefore given Toh's teachings of data exchange between receiver and third party (e.g.,OC) and the receiver ability to perform a hash function, it would have been obvious to those skilled in the art to have a receiver possess the ability to send a copy of a generated hash to a third party to enhance the message (e.g., second hash value) authentication process.

9. As to claim 68 , Toh teaches a method where the first secret key is symmetric and the second secret key is asymmetric (i.e., .. teaches the use of both symmetric and asymmetric keys [par. 28 & 29]).

10. Claims 69-72 (Cancelled)

Response to Arguments

Examiner Remarks – 112th 1st Paragraph Rejection

The Examiner finds applicant's remarks persuasive and therefore withdraws the rejection made under 112th 1st paragraph for claims 63, 67, 69 and 72.

Examiner Remarks – 103(a) Toh in view of Harber

The applicant argues: the following: "In contrast, the present invention of claim 63 involves transmission to a remote location of a single hash value derived from hash values for a plurality of stored data items, whereas Haber transmits to a remote location only a single hash value for particular document",

The Examiner respectfully submits that Harber discloses the following: "…the service bureau takes from R hash value a.sub.5 (FIG. 2B) of document F and combines (e.g., concatenates) that value with the hash value a.sub.6 of a second document which is the subject matter of a second request for certification. At step 14, the service bureau hashes the composite to create a new hash value linked to hash values a.sub.5 and a.sub.6 by a one-way hash function". Harber further discloses MD5 hash values for the repository of FIG. 3. Harber further discloses "…the service bureau calculates a "self-verifying" hash values and the location values (e.g., "handedness") of the self-verifying hash values for the subject document similar to step 17 of FIG. 1. At step 48, the service bureau combines location values and an identifier for root D.sub.1-8 to

form a composite similar to FIG. 1. At optional step 49, the unique name generated by step 48 can be further abbreviated to form an even shorter "nickname" similar to FIG 1. “. Additionally, Harber discloses: “the service bureau transmits the "name" back to the requester. …. the name comprises the combination (e.g., concatenation) of location values (e.g., handedness values) with a root identifier (e.g., a root identifier by the time it was published: "Aug. 18, 1994 7:37:25 AM EDT")”.

The Examiner contends in this instance Harber contemplates creating a hash representative of multiple documents by disclosing the process of hashing document F with a secondary document. The Examiner further submits Harber contemplates sending a hash respective of a plurality of documents by disclosing that the service bureau will transmit to the client the hash representative value. Therefore in view of the cited teachings of Harber the Examiner finds applicant's arguments to be non-persuasive.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory

action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431
/Syed Zia/
Primary Examiner, Art Unit 2431